# Factor-4 and 6 (De)compression for Values of Pairings using Trace Maps*

Tomoko Yonemura, Taichi Isogai, Hirofumi Muratani, and Yoshikazu Hanatani

Toshiba Corporation,
1, Komukai-Toshiba-cho, Saiwai-ku, Kawasaki, 212-8582, Japan
{tomoko.yonemura,taichi1.isogai,hirofumi.muratani,
yoshikazu.hanatani}@toshiba.co.jp

**Abstract.** The security of pairing-based cryptosystems relies on the hardness of the discrete logarithm problems in elliptic curves and in finite fields related to the curves, namely, their embedding fields. Public keys and ciphertexts in the pairing-based cryptosystems are composed of points on the curves or values of pairings. Although the values of the pairings belong to the embedding fields, the representation of the field is inefficient in size because the size of the embedding fields is usually larger than the size of the elliptic curves. We show factor-4 and 6 compression and decompression for the values of the pairings with the supersingular elliptic curves of embedding degrees 4 and 6, respectively. For compression, we use the fact that the values of the pairings belong to algebraic tori that are multiplicative subgroups of the embedding fields. The algebraic tori can be expressed by the affine representation or the trace representation. Although the affine representation allows decompression maps, decompression maps for the trace representation has not been known. In this paper, we propose a trace representation with decompression maps for the characteristics 2 and 3. We first construct efficient decompression maps for trace maps by adding extra information to the trace representation. Our decompressible trace representation with additional information is as efficient as the affine representation is in terms of the costs of compression, decompression and exponentiation, and the size.

**Keywords:** public-key cryptosystems, the discrete logarithm problem, algebraic tori, compression, decompression

## 1 Introduction

Practical public-key cryptography is fundamental technology in the field of network security. Current security standards recommend the use of

* This paper is the full version of [Yonemura, T., Isogai, T., Muratani, H., Hanatani, Y.: Factor-4 and 6 (De)compression for Values of Pairings using Trace Maps. In: Pairing2012 (2012)].

2048-bit or larger RSA keys [2] and history in these decades suggests that this figure may increase with advances in computational power. Such key sizes are problematic for devices with limited storage, computational power or network bandwidth. One approach to overcome these limitations is a safe key compression [20, 6, 14, 16, 5, 19, 12, 13], but these compression techniques are unsuited to RSA keys. Therefore, we focus on cryptosystems based on the discrete logarithm problem in a prime-order group. To compress the public-key size is to represent the prime-order group with fewer bits than the size of the embedding field. For instance, the recommended size of the finite field is 2048 bits, and the corresponding size of the prime-order group is 224 bits [2], because the discrete logarithm problem in the finite field is easier than in the general group, namely, the elliptic curve.

The index calculus is a relatively efficient algorithm to solve the discrete logarithm problem in finite fields. The time complexity of the index calculus is subexponential $L_q[1/3, c] = \exp((c+o(1))(\log q)^{1/3}(\log\log q)^{2/3})$ for the finite field $\mathbb{F}_q$, and does not depend on the characteristic or the extension degree [7, 1, 10, 11] except the constant $c$. On the other hand, there are only exponential algorithms for solving the discrete logarithm problem in the elliptic curves.

Pairings map a pair of elliptic curve points to an element of the multiplicative group of a finite field, namely, the curve's embedding field. Since pairings are bilinear, the discrete logarithm problem in elliptic curves is also solved in their embedding fields. The bilinearity is used to develop efficient cryptographic schemes [18, 9, 3]. In pairing-based cryptosystems, we deal with both rational points of elliptic curves and values of pairings. Although the values of the pairings belong to the embedding fields, the representation of the field is inefficient in the size. We show factor-4 and 6 compression and decompression for the values of the pairings with the supersingular elliptic curves of embedding degrees 4 and 6, respectively. For compression, we use the fact that the values of the pairings belong to also algebraic tori that are the multiplicative subgroups of the embedding fields.

*Related Work.* Table 1 presents existing compression methods. There are two kinds of compression methods: the affine representation and the trace representation. Algebraic tori ($\mathbb{T}_2$, $\mathbb{T}_6$, LUC, XTR) and their subgroups (Karabina, Shirase) have compact expressions.

In the affine representation, elements of algebraic tori are embedded in extension fields and identified by an element / elements from subfields.

**Table 1.** compression methods:ECC, FFC and ATC mean the elliptic curve cryptosystems, the finite field cryptosystems and the algebraic torus cryptosystems, respectively.

| system | ECC | FFC | ATC | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| class | - | - | the affine representation | | | | the trace representation | | | |
| name | - | - | $\mathbb{T}_2$ | $\mathbb{T}_6$ | Karabina | Karabina | LUC | XTR | Karabina | Shirase |
| factor | - | 1 | 2 | 3 | 4 | 6 | 2 | 3 | 4 | 6 |
| public-key size (bit) | 160 | 1024 | 512 | 341 | 256 | 170 | 512 | 341 | 256 | 170 |
| | 224 | 2048 | 1024 | 683 | 512 | 341 | 1024 | 683 | 512 | 341 |
| | 256 | 3072 | 1536 | 1024 | 768 | 512 | 1536 | 1024 | 768 | 512 |
| reference | - | - | [16] | [16] | [13] | [13] | [20] | [14] | [12] | [19] |
| comp. | - | - | available | | | | available | | | |
| decomp. | - | - | available | | | | no | | | |

Elements of subgroups of algebraic tori are identified by a tuple of an element from subfields and additional information, namely, 1 bit for factor 4 or 1 trit (ternary digit) for factor 6. Each affine representation has efficient inverse map allowing multiplication and exponentiation in the embedding fields.

In the trace representation, elements of algebraic tori or these subgroups are identified by a trace value. Because conjugates are mapped to a same trace value, no inverse map exists. Therefore, multiplication could not be defined in the trace representation. On the other hand, exponentiation can be calculated without decompression or without distinction among conjugates. Although Karabina discusses "decompression" without distinction among conjugates, no efficient "decompression" maps are presented [12]. Most cryptosystems use not only exponentiation but also multiplication. The existing trace representation is not useful because of lack of multiplication.

*Our Contributions.* We propose factor-4 and 6 decompressible trace representation with additional information for characteristics 2 and 3, respectively. We construct decompression maps for the trace representation by adding extra information. Our decompression maps are efficient. Since our representation permits decompression, we are able to introduce multiplication in the trace representation for the first time. All cryptographic protocols based on group law and the discrete logarithm problem can be implemented on this representation. Why do we focus not on the affine representation, but on the trace representation? One of the reasons is the trace representation seems to be suited to improving the compression factor.

There are two steps for the construction of our representation: Firstly, we find easily solvable equations whose coefficients are written by the trace value to obtain the elements of the algebraic tori in the embedding fields as solutions. Secondly, we distinguish these solutions by additional information, namely, 2 bits for factor 4 or 1 bit and 1 trit for factor 6.

In order to improve the compression factor, it is required that the tuple of a trace value and additional information have to achieve a better compression factor than Bosma's conjecture. Bosma's conjecture on generalization of XTR mentioned the tuple of a trace value and other fundamental symmetric polynomials to improve the compression factor [4]. However, the additional information is much smaller than the fundamental symmetric polynomials.

*Structure of This Paper.* In section 2 and 3, we present the necessary preliminaries and literature review respectively. In section 4, we propose decompression maps for the trace representation with additional information. In section 5, we compare the efficiency of our representation with existing affine representation.

## 2 Preliminaries and Notation

Let $p$ be a prime, and $n$, $m$ and $d$ be positive integers. Let $\mathbb{F}_{p^m}$ be a finite field of order $p^m$. $I_d$, $M_d$, and $S_d$ are costs of inversion, multiplication, and square in the field $\mathbb{F}_{(p^m)^d}$. We ignore costs of Frobenius maps and addition in $\mathbb{F}_{(p^m)^d}$ that are small compared with the above costs. Maps $Tr_{\mathbb{F}_{(p^m)^n}/\mathbb{F}_{(p^m)^d}}$ and $N_{\mathbb{F}_{(p^m)^n}/\mathbb{F}_{(p^m)^d}}$ denote a trace map and a norm map from $\mathbb{F}_{(p^m)^n}$ to $\mathbb{F}_{(p^m)^d}$, respectively, where, $d$ divides $n$. Maps $Tr_{n/d}$ and $N_{n/d}$ are short for the above maps.

**Definition 1.** *An algebraic torus $\mathbb{T}_n$ over $\mathbb{F}_{p^m}$ is defined by*

$$\mathbb{T}_n(\mathbb{F}_{p^m}) = \bigcap_{\mathbb{F}_{p^m} \subset F \subsetneq \mathbb{F}_{(p^m)^n}} \mathrm{Ker}\left[N_{\mathbb{F}_{(p^m)^n}/F}\right] \ . \tag{1}$$

**Definition 2.** *Let $\mu$ be the Möbius function. The $n$-th cyclotomic polynomial $\Phi_n(x)$ is defined by $\Phi_n(x) = \prod_{d|n}(x^d - 1)^{\mu(n/d)}$.*

**Theorem 1.** *(a) $\#\mathbb{T}_n(\mathbb{F}_{p^m}) = \Phi_n(p^m)$.*
*(b) If $h \in \mathbb{T}_n(\mathbb{F}_{p^m})$ has a prime order not dividing $n$, then $h \notin \mathbb{F}_{(p^m)^d}$ for any $d|n$ with $d < n$.*

*Proof.* (a) Note that $F$ can be $\mathbb{F}_{(p^m)^d}$ for any $d|n$ with $d < n$. See also [16].

(b) Let prime $r$ be the order of $h$. Since $r \not| n$, $X^n - 1$ has no repeated roots in the algebraic closure of $\mathbb{F}_r$. See also [4]. □

In the case of $m > 1$, $\#\mathbb{T}_{mn}(\mathbb{F}_p) = \Phi_{mn}(p)$. If $h \in \mathbb{T}_{mn}(\mathbb{F}_p)$ has a prime order not dividing $mn$, then $h \notin \mathbb{F}_{p^d}$ for any $d|mn$ with $d < mn$. On the other hand, the order of the finite field $\mathbb{F}_{(p^m)^n}$ is factored as in eq. (2) by using cyclotomic polynomials.

$$(p^{mn} - 1) = \prod_{d|mn} \Phi_d(x) \tag{2}$$

The secure subgroup of the multiplicative group $\mathbb{F}^{\times}_{(p^m)^n}$ is not covered in proper subfield $\mathbb{F}_{p^d}$. In other words, it is a subgroup of $\mathbb{T}_{mn}(\mathbb{F}_p)$, and is not a subgroup of $\mathbb{T}_d(\mathbb{F}_p)$. Therefore, public-key cryptosystems defined on prime-order subgroup not dividing $mn$ of the algebraic tori $\mathbb{T}_{mn}(\mathbb{F}_p)$ have the same security level as the multiplicative group $\mathbb{F}^{\times}_{(p^m)^n}$.

Let $E$ be an elliptic curve defined over $\mathbb{F}_{p^m}$, and let $r$ be a positive integer such that $r|\#E(\mathbb{F}_{p^m})$. A subgroup of $E(\mathbb{F}_{p^m})$ with order $r$ has the embedding degree $k$, and $k$ is the smallest integer such that $r|\{(p^m)^k - 1\}$. The Tate pairing is a function

$$\langle \cdot, \cdot \rangle_r : E(\mathbb{F}_{p^m})[r] \times E(\mathbb{F}_{(p^m)^k})/rE(\mathbb{F}_{(p^m)^k}) \to \mathbb{F}^{\times}_{(p^m)^k}/\{\mathbb{F}^{\times}_{(p^m)^k}\}^r.$$

A value of the Tate pairing is an equivalence class in $\mathbb{F}^{\times}_{(p^m)^k}/\{\mathbb{F}^{\times}_{(p^m)^k}\}^r$. For practical purposes, we obtain the reduced Tate pairing $e(P,Q) = \langle P, Q \rangle_r^{\{(p^m)^k - 1\}/r} \in \mu_r \subset \mathbb{F}^{\times}_{(p^m)^k}$ as a unique representative of this class, where $\mu_r$ is a set of $r$-th roots of unity. There is an important fact $\mu_r \subset \mathbb{T}_k(\mathbb{F}_{p^m}) \subset \mathbb{F}^{\times}_{(p^m)^k}$. By definition of the embedding degree, $r \not| \{(p^m)^d - 1\}$ with $d < k$. In other words, $\mu_r$ is a subgroup of $\mathbb{T}_k(\mathbb{F}_{p^m})$, and is not a subgroup of $\mathbb{T}_d(\mathbb{F}_{p^m})$.

The supersingular elliptic curves over $\mathbb{F}_{p^m}$ have the following order [15]. For embedding degree $k = 4$,

- $p = 2$ and $E_i : y^2 + y = x^3 + x + a_i$, where $a_1 = 0$ and $a_2 = 1$.
- $\#E_i(\mathbb{F}_{p^m}) = p^m \pm \sqrt{2p^m} + 1$, where $m$ is odd.

For embedding degree $k = 6$,

- $p = 3$ and $E_i : y^2 = x^3 - x + a_i$, where $a_1 = 1$ and $a_2 = -1$.
- $\#E_i(\mathbb{F}_{p^m}) = p^m \pm \sqrt{3p^m} + 1$, where $m$ is odd.

# 3 Literature review

## 3.1 The Affine Representation

In this section, we recall the definition of $\mathbb{T}_2$. We use the $\mathbb{T}_2$ affine representation as the special case of the projective representation for the following construction of decompression for trace maps. Because operations are more efficient in the projective representation than the affine representation, operations are done in the projective representation. Maps between the affine representation and the projective representation are called a compression map and a decompression map.

$\mathbb{T}_2$. This is the factor-2 compression and decompression method by Rubin and Silverberg. An element of $\mathbb{T}_2(\mathbb{F}_{p^m})$ is identified by an element of $\mathbb{F}_{p^m}$. Let an element $\frac{a+b\sigma}{a+b\sigma^{p^m}}$ of $\mathbb{T}_2(\mathbb{F}_{p^m})$ be corresponding to $(a, b)$. Where $a, b \in \mathbb{F}_{p^m}$ and $(a, b) \neq (0, 0)$, $\mathbb{F}_{(p^m)^2} = \mathbb{F}_{p^m}(\sigma)$, and $\sigma \in \mathbb{F}^{\times}_{(p^m)^2}$. This representation has a natural projective equivalence relation. The element corresponding to $(a, b)$ is equivalent to the element corresponding to $(ac, bc)$ for any $c \in \mathbb{F}^{\times}_{p^m}$. So, this representation can be called the projective representation. We obtain $(a/b, 1)$ as the representative point of $(a, b)$ and it is the affine representation of $\mathbb{T}_2(\mathbb{F}_{p^m})\backslash\{1\}$.

The compression map (from the projective representation to the affine representation) $\mathcal{C}$ and the decompression map (from the affine representation to the projective representation) $\mathcal{D}$ are as follows:

$$\begin{aligned} \mathcal{C} : \mathbb{T}_2(\mathbb{F}_{p^m})\backslash\{1\} &\to \mathbb{F}_{p^m} \quad & \mathcal{D} : \mathbb{F}_{p^m} &\to \mathbb{T}_2(\mathbb{F}_{p^m})\backslash\{1\} \\ \frac{a+b\sigma}{a+b\sigma^{p^m}} &\mapsto a/b, & a' &\mapsto \frac{a'+\sigma}{a'+\sigma^{p^m}}. \end{aligned}$$

## 3.2 The Trace Representation –Compression by Trace Maps

In this section, we explain LUC, Karabina and Shirase. We construct decompression maps for the compression in the next section. Note that exponentiation in the trace representation itself can be calculated, but multiplication is not done.

*LUC.* This is the factor-2 compression method by Smith and Skinner. An element of $\mathbb{T}_2/S_2(\mathbb{F}_{p^m})$ is identified by an element of $\mathbb{F}_{p^m}$. The compression map is as follows:

$$\begin{aligned} Tr_{2/1} : \mathbb{F}_{(p^m)^2} &\to \mathbb{F}_{p^m} \\ g &\mapsto g + g^{p^m}. \end{aligned}$$

In the trace representation, an element $g$ and its conjugate $g^{p^m}$ have the same trace value. Let $S_d$ denote symmetric group of degree $d$, which is a set of all bijections in $\{0, 1, \cdots, d-1\}$. It is shown that $\mathbb{T}_2/S_2$ is rational on $\mathbb{F}_{p^m}$ [17]. The inverse map from $\mathbb{A}$ to $\mathbb{T}_2/S_2$ implies that $g \in \mathbb{T}_2(\mathbb{F}_{p^m})$ has no element which has the same trace value $Tr_{2/1}(g)$ without conjugate $g^{p^m}$. the trace value $Tr_{2/1}(g)$ is only for $g \in \mathbb{T}_2(\mathbb{F}_{p^m})$ and the conjugate $g^{p^m}$.

*Karabina.* This is the factor-4 compression method. Let $p = 2$ and $m$ be odd. An element of groups $G_\pm$, $\#G_\pm = p^m \pm \sqrt{2p^m} + 1$, is identified by an element of $\mathbb{F}_{p^m}$ without distinction among conjugates. The compression map is as follows:

$$\begin{aligned} Tr_{4/1} : \mathbb{F}_{(p^m)^4} &\to \mathbb{F}_{p^m} \\ g &\mapsto g + g^{p^m} + g^{(p^m)^2} + g^{(p^m)^3}. \end{aligned}$$

Since $\#G_+ \#G_- = \Phi_4(p^m)$, The groups $G_\pm$ are subgroups of $\mathbb{T}_4(\mathbb{F}_{p^m})$. Such subgroups are related to supersingular elliptic curves of embedding degree 4. Karabina also proposed some exponentiation formulas. Although there is "decompression" without distinction between conjugates, he didn't give any efficient decompression maps.

*Shirase.* This is the factor-6 compression method. Let $p = 3$ and $m$ be odd. An element of groups $G_\pm$, $\#G_\pm = p^m \pm \sqrt{3p^m} + 1$, is identified by an element of $\mathbb{F}_{p^m}$ without distinction among conjugates. The compression map is as follows:

$$\begin{aligned} Tr_{6/1} : \mathbb{F}_{(p^m)^6} &\to \mathbb{F}_{p^m} \\ g &\mapsto g + g^{p^m} + g^{(p^m)^2} + g^{(p^m)^3} + g^{(p^m)^4} + g^{(p^m)^5}. \end{aligned}$$

Since $\#G_+ \#G_- = \Phi_6(p^m)$, The groups $G_\pm$ are subgroups of $\mathbb{T}_6(\mathbb{F}_{p^m})$. Such subgroups are related to supersingular elliptic curves of embedding degree 6.

## 4 Construction of Decompression for Trace Maps

We propose the decompressible trace representation with additional information. The trace representation is decompressed to the projective representation for factor 4 and 6, and then multiplication can be calculated. Therefore, all cryptographic protocols based on group law and the discrete logarithm problem can be implemented on this representation.

### 4.1 Factor 2

We show decompression from $(i, Tr_{2/1}(g)) \in \{0,1\} \times \mathbb{F}_{p^m}$ to $g \in \mathbb{T}_2(\mathbb{F}_{p^m}) \subset \mathbb{F}_{(p^m)^2}$. An important idea is solving condition of the element belongs to the algebraic torus and distinguishing two solutions by using additional information. The point is that we solve the condition for the element in the algebraic torus and distinguish the two solutions by using additional information. We explain the idea in detail. The finite field $\mathbb{F}_{(p^m)^2}$ is constructed as follows: $\mathbb{F}_{(p^m)^2}$ is constructed as follows:

$$\mathbb{F}_{(p^m)^2} = \mathbb{F}_{p^m}[x]/f_2(x),\ f_2(x) = x^2 - c,\ c \in \mathbb{F}_{p^m}^{\times}.$$

When, $g = g_0 + g_1 x$ we obtain $Tr_{2/1}(g) = 2g_0$. Note that $x^{p^m} = -x$. If $g \in \mathbb{T}_2(\mathbb{F}_{p^m})$ then $g^{p^m+1} = 1$. A degree-2 equation $cg_1^2 - g_0^2 + 1 = 0$ is led from $(g_0 - g_1 x)(g_0 + g_1 x) = 1$. Solutions of the above equation are $g_1 = \pm\sqrt{(g_0^2 - 1)/c}$ in $\mathbb{F}_{p^m}$. We obtain $\{g, g^{p^m}\} = \{g_0 + \sqrt{(g_0^2 - 1)/c}x, g_0 - \sqrt{(g_0^2 - 1)/c}x\}$. Therefore, LUC with 1 bit of information added is decompressed for embedding in $\mathbb{F}_{(p^m)^2}$ as follows:

$$\begin{cases} (0, Tr_{2/1}(g)) = Tr_{2/1}(g)/2 + \sqrt{(Tr_{2/1}(g)^2/4 - 1)/c}x, \\ (1, Tr_{2/1}(g)) = Tr_{2/1}(g)/2 - \sqrt{(Tr_{2/1}(g)^2/4 - 1)/c}x. \end{cases}$$

In the above discussion, $g_1$ is identified by root and sign temporarily.

### 4.2 Factor 4

We show decompression from $(i, Tr_{4/1}(g)) \in \{0,1\}^2 \times \mathbb{F}_{p^m}$ to $g \in G_- \subset \mathbb{T}_4(\mathbb{F}_{p^m}) \subset \mathbb{F}_{(p^m)^4}$. Firstly, we find equations to obtain four possible solutions by $Tr_{4/1}(g)$. Secondly, we distinguish the conjugates by the additional information $i$. The finite field $\mathbb{F}_{(p^m)^4}$ is constructed as follows:

- primitive polynomial: $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$,
- basis: $\{x, x^{p^m}, x^{(p^m)^2}, x^{(p^m)^3}\} = \{x, x^2, x^4, x^3\}$.

We use $p^m \bmod 5 = 2$, $z = x + x^{p^m}$ and $y = x + x^{(p^m)^2}$. One can also use $p^m \bmod 5 = 3$.

**Theorem 2.** *Suppose $p = 2$, $m$ is odd, $t = \sqrt{2p^m}$ and $G_-$ is a group of order $p^m - t + 1$, then there exist the compression map $\mathcal{C}$ described by eq. (3) and the decompression map $\mathcal{D}$ described by eq. (4).*

$$\begin{aligned} \mathcal{C} : G_- \backslash \{1\} &\to \{0,1\}^2 \times \mathbb{F}_{p^m} \\ \frac{h}{h^{(p^m)^2}} &\mapsto (i, Tr_{4/1}(g)) \end{aligned} \tag{3}$$

$$\begin{aligned} \mathcal{D} : \{0,1\}^2 \times \mathbb{F}_{p^m} &\to G_-\backslash\{1\} \\ (i, Tr_{4/1}(g)) &\mapsto \frac{f+z}{f+z^{(p^m)^2}} \end{aligned} \tag{4}$$

*Where, the projective representation of $g$ is $\frac{h}{h^{(p^m)^2}}$, $h \in \mathbb{F}_{(p^m)^4}$, and the $\mathbb{T}_2$ affine representation of $g$ is $\frac{f+z}{f+z^{(p^m)^2}}$, $f = \delta_1 y + \delta_2 y^{p^m} \in \mathbb{F}_{(p^m)^2}$ for some $\delta_1$, $\delta_2 \in \mathbb{F}_{p^m}$. Let $i$ be a tuple of the least bits in the vector representation of $\delta_1$ and $\delta_2$.*

*Proof.* The decompression map $\mathcal{D}$ is calculated by solving eq. (5) in Lemma 2 and eq. (6) in Lemma 3. The following Lemma 1 is condition for the element in the subgroup of the algebraic torus, and leads to Lemma 2 and 3. Lemma 4 shows why $i$ distinguishes the four solutions. □

Calculations of the compression map $\mathcal{C}$ and the decompression map $\mathcal{D}$ are shown in Algorithm 1 and 2.

**Algorithm 1** Factor-4 compression $\mathcal{C}$

Input: the projective representation $\frac{h}{h^{(p^m)^2}} = \frac{h_0+h_1 z}{h_0+h_1 z^{(p^m)^2}}$ for $g$
Output: $(i, Tr_{4/1}(g))$

1: $f = \delta_1 y + \delta_2 y^{p^m} \leftarrow h_0/h_1$
2: $i_1 \leftarrow$ the least bit of $\delta_1$ in the vector representation
3: $i_2 \leftarrow$ the least bit of $\delta_2$ in the vector representation
4: $i \leftarrow (i_1, i_2)$
5: $Tr_{4/1}(g) \leftarrow \frac{\delta_1^2+\delta_2^2+\delta_1+\delta_2+1}{\delta_1^4+\delta_1^2\delta_2^2+\delta_2^4+\delta_1^3+\delta_2^3+\delta_1\delta_2+\delta_2^2+\delta_2+1}$

**Algorithm 2** Factor-4 decompression $\mathcal{D}$

Input: $(i, Tr_{4/1}(g))$
Output: the $\mathbb{T}_2$ affine representation $\frac{f+z}{f+z^{(p^m)^2}}$, $f = \delta_1 y + \delta_2 y^{p^m}$ for $g$

1: solve $D^2 + D + 1 = \{Tr_{4/1}(g)\}^{p^m - t}$ for $D$ and obtain a solution $D$ with the least bit $i_1 + i_2$ in the vector representation
2: solve $\delta_2^2 + \delta_2 = D^2 + \{Tr_{4/1}(g)\}^{p^m - t} D^t$ for $\delta_2$ and obtain $\delta_2$ with the least bit $i_2$ in the vector representation
3: $\delta_1 \leftarrow \delta_2 + D$

**Lemma 1.** *Use the notation in Theorem 2. Let $g = \frac{f+z}{f+z^{(p^m)^2}} \in G_-\backslash\{1\}$. When $t \bmod 5 = 2$, $\delta_1$ and $\delta_2$ satisfy*

$$(\delta_1 + \delta_2)^{t+1} = \delta_1^t + \delta_2 + 1.$$

*Proof.* The condition $g \in G_-\backslash\{1\}$ leads to $g^{p^m+1} = g^t$. We substitute $g = \frac{f+z}{f+z^{(p^m)^2}}$ in the above equation, and then

$$\{\delta_1^{t+1} + \delta_1\delta_2^t + \delta_1^t + (\delta_1^2 + \delta_1\delta_2 + \delta_2^2 + \delta_1 + \delta_2^t)\}y \\ + \{\delta_2^{t+1} + \delta_1^t\delta_2 + \delta_2 + 1 + (\delta_1^2 + \delta_1\delta_2 + \delta_2^2 + \delta_1 + \delta_2^t)\}y^{p^m} = 0.$$

We obtain the desired equation from the sum of coefficients for $y$ and $y^{p^m}$. □

**Lemma 2.** *Use the notation in Theorem 2.* $D = \delta_1 + \delta_2 \in \mathbb{F}_{p^m}$ *satisfies*

$$D^2 + D + 1 = \{Tr_{4/1}(g)\}^{p^m - t}. \tag{5}$$

*Proof.* Lemma 1 leads to

$$\begin{cases} \delta_1^2 + \delta_2 = (\delta_1^t + \delta_2^t)(\delta_1^2 + \delta_2^2 + \delta_1 + \delta_2 + 1), \\ \delta_1 + \delta_2^2 = (\delta_1^t + \delta_2^t + 1)(\delta_1^2 + \delta_2^2 + \delta_1 + \delta_2 + 1) + 1. \end{cases}$$

We substitute the above equations to the trace value

$$Tr_{4/1}(g) = \frac{\delta_1^2 + \delta_2^2 + \delta_1 + \delta_2 + 1}{\delta_1^4 + \delta_1^2\delta_2^2 + \delta_2^4 + \delta_1^3 + \delta_2^3 + \delta_1\delta_2 + \delta_2^2 + \delta_2 + 1},$$

and then we obtain

$$(\delta_1^2 + \delta_2^2 + \delta_1 + \delta_2 + 1)^{t+1} = Tr_{4/1}(g)^{-1}.$$

Where $t^2 = 2p^m$ and $\delta_1, \delta_2, Tr_{4/1}(g) \in \mathbb{F}_{p^m}$, we obtain

$$\delta_1^2 + \delta_2^2 + \delta_1 + \delta_2 + 1 = \{Tr_{4/1}(g)\}^{p^m - t}.$$

□

Note that the characteristic is 2, and square is calculated by the Frobenius map involving rotation of elements in the normal basis. We obtain two solutions $D_0$ and $D_1$ of eq. (5) immediately.

**Lemma 3.** *Use the notation in Theorem 2. The element* $\delta_2$ *satisfies*

$$\delta_2^2 + \delta_2 = D^2 + \{Tr_{4/1}(g)\}^{p^m - t}D^t. \tag{6}$$

*Proof.* Lemma 1 leads to

$$\delta_1^2 + \delta_2 = (\delta_1^t + \delta_2^t)(\delta_1^2 + \delta_2^2 + \delta_1 + \delta_2 + 1).$$

We show how to transform the equation of Lemma 1 to the above equation later. The left-hand side of the above equation is $(D + \delta_2)^2 + \delta_2 = D^2 + \delta_2^2 + \delta_2$, and then we obtain eq.(6).

Where $t^2 = 2p^m$ and $\delta_1, \delta_2 \in \mathbb{F}_{p^m}$, the equation of Lemma 1 to the power of $(t-1)$ is

$$(\delta_1 + \delta_2) = (\delta_1^t + \delta_2 + 1)^{t-1},$$

and then we obtain

$$(\delta_1 + \delta_2)(\delta_1^t + \delta_2 + 1) = \delta_1^2 + \delta_2^t + 1.$$

We add $\delta_1^t + \delta_2^t$ to the equation of Lemma 1 multiplied by $\delta_1 + \delta_2 + 1$,

$$(\delta_1^t + \delta_2^t)(\delta_1^2 + \delta_2^2 + \delta_1 + \delta_2 + 1) = (\delta_1 + \delta_2)(\delta_1^t + \delta_2 + 1) + \delta_2^t + \delta_2 + 1.$$

We substitute $(\delta_1 + \delta_2)(\delta_1^t + \delta_2 + 1) = \delta_1^2 + \delta_2^t + 1$ to the above equation, and then we obtain the first equation in this proof. □

We obtain two $\delta_2$ by solving eq. (6) with fixed $D$. Therefore, we obtain four solutions for $(\delta_1, \delta_2)$.

**Lemma 4.** *Use the notation in Theorem 2. The least bits in the vector representation of $\delta_1$ and $\delta_2$ identify $g \in G_- \backslash \{1\}$ from solutions of eq. (5) and (6).*

*Proof.* The element $g$ changes by $p^m$ power: $(\delta_1, \delta_2) \to (\delta_2 + 1, \delta_1) \to (\delta_1 + 1, \delta_2 + 1) \to (\delta_2 + 1, \delta_1)$. □

### 4.3 Factor 6

We show decompression from $(i, Tr(g)) \in \{0,1\} \times \{0,1,2\} \times \mathbb{F}_{p^m}$ to $g \in G_- \subset \mathbb{T}_6(\mathbb{F}_{p^m}) \subset \mathbb{F}_{(p^m)^6}$. Firstly, we find equations to obtain six possible solutions by $Tr_{6/1}(g)$. Secondly, we distinguish the conjugates by the additional information $i$. The finite field $\mathbb{F}_{(p^m)^6}$ is constructed as follows:

- primitive polynomial: $\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$,
- basis: $\{x, x^{p^m}, x^{(p^m)^2}, x^{(p^m)^3}, x^{(p^m)^4}, x^{(p^m)^5}\} = \{x, x^5, x^4, x^6, x^2, x^3\}$.

We use $p^m \bmod 7 = 5$, $z = x + x^{(p^m)^2} + x^{(p^m)^4}$ and $y = x + x^{(p^m)^3}$. One can also use $p^m \bmod 7 = 3$.

**Theorem 3.** *Suppose $p = 3$, $m$ is odd, $t = \sqrt{3p^m}$ and $G_-$ is a group of order $p^m - t + 1$, then there exist the compression map $\mathcal{C}$ described by eq. (7) and the decompression map $\mathcal{D}$ described by eq. (8).*

$$\begin{aligned} \mathcal{C} : G_- \backslash \{1\} &\to \{0,1\} \times \{0,1,2\} \times \mathbb{F}_{p^m} \\ \frac{h}{h^{(p^m)^3}} &\mapsto (i, Tr_{6/1}(g)) \end{aligned} \tag{7}$$

$$\begin{aligned} \mathcal{D} : \{0,1\} \times \{0,1,2\} \times \mathbb{F}_{p^m} &\to G_- \backslash \{1\} \\ (i, Tr_{6/1}(g)) &\mapsto \frac{f+z}{f+z^{p^m}} \end{aligned} \tag{8}$$

*Where, the projective representation of $g$ is $\frac{h}{h^{(p^m)^3}}$, $h \in \mathbb{F}_{(p^m)^6}$, and the $\mathbb{T}_2$ affine representation of $g$ is $\frac{f+z}{f+z^{p^m}}$, $f = \delta_1 y + \delta_2 y^{p^m} + \delta_3 y^{(p^m)^2} \in \mathbb{F}_{(p^m)^3}$ for some $\delta_1$, $\delta_2$, $\delta_3 \in \mathbb{F}_{p^m}$. The bit $\{1,0\}$ is transformed from $\{1,2\}$ of a trit in $A^{-1}$ for $A = \delta_1 + \delta_2 + \delta_3$. The trit is in $\beta'$ calculated from $\delta_2$.*

*Proof.* The decompression map $\mathcal{D}$ is calculated by solving eq. (9) in Lemma 6 and eq. (10) in Lemma 7. The following Lemma 5 is condition for the element in the subgroup of the algebraic torus, and leads to Lemma 6, 7 and 8. Lemma 9 shows why $i$ distinguishes the six solutions. □

Calculations of the compression map $\mathcal{C}$ and the decompression map $\mathcal{D}$ are shown in Algorithm 3 and 4.

**Algorithm 3** Factor-6 compression $\mathcal{C}$

Input: the projective representation $\frac{h}{h^{(p^m)^2}} = \frac{h_0 + h_1 z}{h_0 + h_1 z^{p^m}}$ for $g$
Output: $(i, Tr_{6/1}(g))$

1: $f = \delta_1 y + \delta_2 y^{p^m} + \delta_3 y^{(p^m)^2} \leftarrow h_0/h_1$
2: $\alpha \leftarrow \delta_1 - 1$
3: $\beta \leftarrow \delta_2 - 1$
4: $\gamma \leftarrow \delta_3 - 1$
5: $A \leftarrow \alpha + \beta + \gamma (= \delta_1 + \delta_2 + \delta_3)$
6: $B \leftarrow \alpha\beta^2 + \beta\gamma^2 + \gamma\alpha^2$
7: $C \leftarrow \alpha\beta\gamma$
8: $i_1 \leftarrow a_i \bmod 2$ for $a_i$ that is the smallest nonzero trit of $A^{-1}$ in the vector rep.
9: $\beta' \leftarrow \frac{A^{t+3} + A^2 + 1}{A^{t+1}(A^2 - 1 - A\beta)}$
10: $i_2 \leftarrow$ the least trit of $\beta'$ in the vector representation
11: $i \leftarrow (i_1, i_2)$
12: $Tr_{6/1}(g) \leftarrow \frac{A}{B + C - A^3 - A}$

**Algorithm 4** Factor-6 decompression $\mathcal{D}$

Input: $(i, Tr_{6/1}(g))$

Output: the $\mathbb{T}_2$ affine representation $\frac{f+z}{f+z^{p^m}}$, $f = \delta_1 y + \delta_2 y^{p^m} + \delta_3 y^{(p^m)^2}$ for $g$

1: solve $A^{-2} = -[\{Tr_{6/1}(g)\}^{t-2} + 1]$ for $A^{-1}$ and obtain solutions $A_0^{-1}, A_1^{-1}$
2: **if** $i_1 = 1$ **then**
3: select $A_1^{-1}$ with $a_i = 1$ for the least nonzero trit $a_i$ in the vector representation
4: **else if** $i_1 = 0$ **then**
5: select $A_0^{-1}$ with $a_i = 2$ for the least nonzero trit $a_i$ in the vector representation
6: **end if**
7: solve $\beta'^3 - \beta' - (\frac{A^2+1}{A^{t+3}} + 1) = 0$ and obtain a solution $\beta'$ with the least trit $i_2$
8: $\beta \leftarrow -A\{(\frac{A^2+1}{A^{t+3}} + 1)\frac{1}{\beta'} + 1 - A^{-2}\}$
9: $t_b \leftarrow -(1 + A^{-2})A^{-t} - A^{-1}$
10: $t_c \leftarrow A^2 - At_b + A^{-1}t_b - t_b^2 - A^{-4}$
11: $\gamma \leftarrow \frac{(1-A^{-2})\beta^2 + t_b\beta - t_c}{-A^{-1}\beta^2 + (1-A^{-2})\beta}$

**Lemma 5.** *Use the notation in Theorem 3. Let* $g = \frac{f+z}{f+z^{p^m}}$. *Note* $z^{(p^m)^3} = z^{p^m}$. *When* $m \bmod 12 = 5$, $\delta_1$, $\delta_2$ *and* $\delta_3$ *satisfy*

$$\delta_1^t(\delta_3 - \delta_2) + \delta_3^t(\delta_1 + \delta_2 + \delta_3) + 2\delta_3\delta_1 + \delta_1\delta_2 + \delta_1^2 + \delta_2^2 - \delta_3 = 2,$$
$$\delta_2^t(\delta_1 - \delta_3) + \delta_1^t(\delta_1 + \delta_2 + \delta_3) + 2\delta_1\delta_2 + \delta_2\delta_3 + \delta_2^2 + \delta_3^2 - \delta_1 = 2,$$
$$\delta_3^t(\delta_2 - \delta_1) + \delta_2^t(\delta_1 + \delta_2 + \delta_3) + 2\delta_2\delta_3 + \delta_3\delta_1 + \delta_3^2 + \delta_1^2 - \delta_2 = 2.$$

*Proof.* $g \in G_-\backslash\{1\}$ leads to $g^{p^m+1} = g^t$. We substitute $g = \frac{f+z}{f+z^{(p^m)^2}}$ in $g^{p^m+1} = g^t$, and then we obtain the desired equations from coefficients for $y$, $y^{p^m}$ and $y^{(p^m)^2}$. □

**Lemma 6.** *Use the notation in Theorem 3. Let* $\alpha = \delta_1 - 1$, $\beta = \delta_2 - 1$, $\gamma = \delta_3 - 1$, $A = \alpha + \beta + \gamma$, $B = \alpha\beta^2 + \beta\gamma^2 + \gamma\alpha^2$ *and* $C = \alpha\beta\gamma$, *where,* $\alpha, \beta, \gamma, A, B, C \in \mathbb{F}_{p^m}$. $A$ *satisfies*

$$A^{-2} = -[\{Tr_{6/1}(g)\}^{t-2} + 1]. \tag{9}$$

*Where* $B = ((-1 - A^2)/A^t) - A$ *and* $C = A^3 - B + (AB - B^2 - 1)/A^3$.

*Proof.* We substitute the equations of Lemma 5 to the trace value

$$Tr_{6/1}(g) = \frac{A}{B + C - A^3 - A},$$

and then we obtain eq. (9). □

Two solutions $A_0$ and $A_1$ of eq. (9) are calculated by square root.

**Lemma 7.** *Use the notation in Theorem 3. The element $\beta$ satisfies*

$$\beta^3 - A\beta^2 - (A^2 - 1)\beta - C = 0. \tag{10}$$

*Proof.* $g \in \mathbb{T}_2(\mathbb{F}_{(p^m)^3})$ leads $\alpha^2 + \beta^2 + \gamma^2 = 1$. Eq. (10) is obtained from the above equation, $B = ((-1 - A^2)/A^t) - A$ and $C = A^3 - B + (AB - B^2 - 1)/A^3$. □

We obtain three $\beta$ by solving eq. (10).

**Lemma 8.** *Use the notation in Theorem 3. The element $\gamma$ satisfies*

$$(-A\beta^2 + (A^2 - 1)\beta)\gamma + (-A^2 + 1)\beta^2 - B\beta + AC = 0. \tag{11}$$

*Proof.* Eq. (11) is obtained from $\alpha^2 + \beta^2 + \gamma^2 = 1$.

We obtain $\gamma$ by solving eq. (11). Therefore we obtain six solutions for $(\delta_1, \delta_2, \delta_3)$.

**Lemma 9.** *Use the notation in Theorem 3. The additional information $i = (i_1, i_2)$ identify $g \in G_-\backslash\{1\}$ from solutions of eq. (9) and eq. (10). Let $i_1 = a_i \bmod 2$ for the least nonzero trit $a_i$ of $A^{-1}$, and $i_2$ be the least trit of $\beta' = \frac{A^{t+3}+A^2+1}{A^{t+1}(A^2-1-A\beta)}$ in the vector representation.*

*Proof.* A trit of $A_0^{-1}$ and a trit of $A_1^{-1}$ in the same place are different unless the trit is zero because of $A_1^{-1} = -A_0^{-1}$. Solutions of the degree-3 equation are $\{\beta'_0, \beta'_0 + 1, \beta'_0 - 1\}$, and then trits of these solutions are different in all places. □

## 5 Performance

In this section, we compare costs of compression, decompression and exponentiation in our representation with existing schemes using the affine representation. We summarize our findings first and then present the detailed calculations.

Table 2 shows that compression and decompression costs are comparable. Note that the cost of solving the equation $X^p \pm X + C = 0$ is negligible, where $X, C \in \mathbb{F}_{p^m}$, $C$ is constant. Exponentiation costs are the same, because we can use the projective representation and store precomputed information in the $\mathbb{T}_2$ affine representation. In the future, there is hope to improve upon naive exponentiation in the trace representation by using precomputation. The size of the additional information is comparable. We consider the computations of our representation with the compression factor of 4 and 6 in detail.

**Table 2.** costs: let $M_6 = 18M_1$, $M_4 = 9M_1$, $M_3 = 6M_1$, $M_2 = 3M_1$ (by Karatsuba's method), $S_6 = M_6$, $S_1 = M_1$ (for simplicity), $I_3 = I_1 + 3M_3$ and $I_2 = I_1 + 2M_2$ (by Itoh-Tsujii's method [8]). $SqRt = \{\log_2 \frac{m-1}{2} + HW(\frac{m-1}{2})\}M_1 + S_1$ [12].

| class | the affine representation | | the trace representation | |
|---|---|---|---|---|
| name | Karabina | Karabina | this work | this work |
| factor | 4 | 6 | 4 | 6 |
| comp. | $I_1 + 9M_1$ | $I_1 + 24M_1$ | $2I_1 + 16M_1$ | $2I_1 + 44M_1$ |
| decomp. | $3M_1$ | $I_1 + 9M_1$ | $I_1 + 3M_1$ | $4I_1 + SqRt + 15M_1$ |
| exp. | $\frac{6}{w+1}\log_2 rM_1$ | $\frac{24}{2w+1}\log_3 rM_1$ | $\frac{6}{w+1}\log_2 rM_1$ | $\frac{24}{2w+1}\log_3 rM_1$ |
| added info. | 1 bit | 1 trit | 2 bits | 1 bit and 1 trit |

*Factor 4.* The compression map $\mathcal{C}$ described by eq. (3) costs $I_2+I_1+M_2+4M_1$ to calculate $f$ for $i$ and $Tr_{4/1}$. Alternatively, we can also calculate $Tr_{4/1}$ using $h$ rather than $f$. In this case, $\mathcal{C}$ costs $I_2 + M_4 + S_4 + 4M_2 + 6M_1 \sim I_1 + 42M_1$. The decompression map $\mathcal{D}$ described by eq. (4) costs $I_1 + 2M_1 + S_1$ to calculate the coefficient of eq. (5) and eq. (6).

Because the image of the decompression map is in the projective representation in both cases of the affine representation and our representation, operations are calculated similarly. There is an exponentiation formula for the trace representation [12]. Its cost is estimated to be $(4M_1+1S_1)\log_2 r$, which is efficient compared with cost of simple square and multiplying $(M_4+S_4)\log_2 r$. However, this is inefficient compared with cost of width-$w$ NAF in the projective representation.

*Factor 6.* The compression map $\mathcal{C}$ described by eq. (7) costs $I_3+I_1+M_3+18M_1+2S_1$ to calculate $f$ and $A^{-1}$ for $i$ and also to calculate $Tr_{6/1}$. Where, $A^{-1}$, $\{A^{t+1}(A^2-1-A\beta)\}^{-1}$ and $(B+C-A^3-A)^{-1}$ can be calculated by one inversion of the product $A\cdot\{A^{t+1}(A^2-1-A\beta)\}\cdot(B+C-A^3-A)$ in Algorithm 3. The decompression map $\mathcal{D}$ described by eq. (8) costs $4I_1+SqRt+10M_1+5S_1$ to perform the following calculations: to calculate the coefficient of eq. (9) and the square root, to solve degree-3 equation, to transform the solution and to calculate $\gamma$. We explain solving degree-3 equation in detail. Let $\beta = -A\{(\frac{A^2+1}{A^{t+3}}+1)\frac{1}{\beta'} + \frac{A^2-1}{A^2}\}$, then eq. (10) is written $\beta'^3 - \beta' - (\frac{A^2+1}{A^{t+3}}+1) = 0$ by using $\beta'$. Note that the characteristic is 3, cubing is calculated by the Frobenius map involving rotation of elements in the normal basis. We obtain three solutions $\beta'$ of the above equation immediately. One calculates the coefficient of the above equation and the transformation from $\beta'$ for $\beta$.

The cost of an exponentiation formula for the trace representation [12] is estimated to be $(23M_1 + S_1)\log_3 r$, which is efficient compared with

cost of simple cubing and multiplying $(2M_6 + C_6) \log_3 r$. However, this is inefficient compared with cost of width-$w$ radix-3 NAF in the projective representation.

## 6 Conclusion

In this paper, we proposed the factor-4 and 6 decompressible trace representation with additional information for the characteristics 2 and 3, respectively. This representation has an efficient decompression map for the trace representation distinguishing conjugates by using the additional information. Since this representation permits decompression, we succeed in introducing multiplication in the trace representation for the first time. Practically, this representation is not worse than the affine representation. Although compression and decompression incur some extra field inversions in comparison with the affine representation, this fact is not a serious disadvantage of the proposed representation because the costs of compression and decompression is much smaller than the costs of encryption and decryption. It is clear that the cost of inversion in the base field is much smaller than the cost of exponentiation in the embedding field. In future work, we intend to improve the compression factor and reduce costs for the exponentiation, the compression and the decompression.

## References

1. Adleman, L.M.: The Function Field Sieve. In: ANTS-I. LNCS, vol. 877, pp. 108–121. Springer-Verlag (1994)
2. Barker, E., Barker, W., Burr, W., Polk, W., Smid, M.: Recommendation for Key Management - Part 1: Genaral (Revised). Special Publication 800/57, NIST (2007)
3. Boneh, D., Franklin, M.: Identity Based Encryption from Weil Pairing. In: CRYPTO2001. LNCS, vol. 2139, pp. 213–220. Springer-Verlag (2001)
4. Bosma, W., Hutton, J., Verheul, E.R.: Looking beyond XTR. In: ASIACRYPT2002. LNCS, vol. 2501, pp. 321–332. Springer-Verlag (2002)
5. Giuliani, K.J., Gong, G.: Efficient Key Agreement and Signature Schemes Using Compact Representations in GF($p^{10}$). In: ISIT2004. pp. 13–13. IEEE (2004)
6. Gong, G., Harn, L.: Public-key Cryptosystems besed on Cubic Finite Field Extensions. IEEE Trans. Inform. Theory 45, 2601–2605 (1999)
7. Gordon, D.: Discrete Logarithms in GF($p$) Using the Number Field Sieve. SIAM J. on Discrete Math. 6, 124–138 (1993)
8. Itoh, T., Tsujii, S.: A Fast Algorithm for Computing Multiplicative Inverses in GF($2^m$) Using Normal Bases. Information and Computation 78(3), 171–177 (1988)
9. Joux, A.: A One Round Protocol for Tripartite Diffie-Hellman. In: ANTS-IV. LNCS, vol. 1838, pp. 385–394. Springer-Verlag (2000)
10. Joux, A., Lercier, R.: The Function Field Sieve in the Medium Prime Case. In: EUROCRYPT2006. LNCS, vol. 4004, pp. 254–270. Springer-Verlag (2006)

11. Joux, A., Lercier, R., Smart, N.P., Vercauteren, F.: The Number Field Sieve in the Medium Prime Case. In: CRYPTO2006. LNCS, vol. 4117, pp. 326–344. Springer-Verlag (2007)
12. Karabina, K.: Factor-4 and 6 Compression of Cyclotomic Subgroups. J. of Mathematical Cryptology 4(1), 1–42 (2010)
13. Karabina, K.: Torus-based Compression by Factor 4 and 6. Cryptology ePrint Archive, Report 2010/525 (2010)
14. Lenstra, A.K., Verheul, E.R.: The XTR Public Key System. In: CRYPTO2000. LNCS, vol. 1880, pp. 1–19. Springer-Verlag (2000)
15. Miyaji, A., Nakabayashi, M., Takano, S.: New Explicit Conditions of Elliptic Curve Traces for FR-Reduction. IEICE Trans. E84-A(5), 1234–1243 (2001)
16. Rubin, K., Silverberg, A.: Torus-based Cryptography. In: CRYPTO2003. LNCS, vol. 2729, pp. 349–365. Springer-Verlag (2003)
17. Rubin, K., Silverberg, A.: Compression in Finite Fields and Torus-based Cryptography. SIAM J. on Computing 37(5), 1401–1428 (2008)
18. Sakai, R., Ohgishi, K., Kasahara, M.: Cryptsystems based on Pairing. In: SCIS2000 (2000)
19. Shirase, M., Han, D., Hibino, Y., Kim, H., Takagi, T.: A More Compact Representation of XTR Cryptosystem. IEICE Trans. E91-A(10), 2843–2850 (2008)
20. Smith, P., Skinner, C.: A Public-key Cryptosystem and a Digital Signature Based on the Lucas Function Analogue to Discrete Logarithms. In: ASIACRYPT1994. LNCS, vol. 917, pp. 357–364. Springer-Verlag (1995)

## A The Affine Representation

Compression and decompression costs of the affine representation [13] are calculated as follows.

*Factor 4.* The point is that the condition for the element in the subgroup of the algebraic torus $\mathbb{T}_n(\mathbb{F}_{p^m})$ is solved and $n/2$ solutions are distinguished by using additional information in the $\mathbb{T}_2$ affine representation. The order of the subgroups is $\#G_{\pm} = p^m \pm t + 1, t = \sqrt{2p^m}$, where, $p = 2$, $m$ is odd.

The compression map $\mathcal{C}$ is described by eq. (12) and the decompression map $\mathcal{D}$ is described by eq. (13). Where, $G \in \{G_-, G_+\}$.

$$\begin{aligned} \mathcal{C} : G\backslash\{1\} &\to \{0,1\} \times \mathbb{F}_{p^m} \\ \frac{\alpha + \beta\sigma}{\alpha + \beta(1+\sigma)} &\mapsto (i, b) \end{aligned} \tag{12}$$

$$\begin{aligned} \mathcal{D} : \{0,1\} \times \mathbb{F}_{p^m} &\to G\backslash\{1\} \\ (i, b) &\mapsto \frac{(a + bw) + \sigma}{(a + bw) + 1 + \sigma} \end{aligned} \tag{13}$$

Let $\mathbb{F}_{(p^m)^4} = \mathbb{F}_{(p^m)^2}(\sigma)$, $\mathbb{F}_{(p^m)^2} = \mathbb{F}_{p^m}(w)$, $\sigma \in \mathbb{F}_{(p^m)^4}$, $w \in \mathbb{F}_{(p^m)^2}$. We obtain $a, b \in \mathbb{F}_{p^m}$ by $\alpha/\beta = a + bw$ from $\alpha, \beta \in \mathbb{F}_{(p^m)^2}$. We calculate roots

of polynomial $P_1(x,b) = x^t + x + u(b) \in \mathbb{F}_{p^m}[x]$ led by $g^{p^m \pm t+1} = 1$ in order to obtain $a$ from $b$. If the above polynomial $P_1(x)$ has two distinct roots $a_0$ and $a_1$, then $a_1 = a_0 + 1$. Note that if the characteristic is 2, solving $P_1(x) = 0$ is easy. The additional information $i$ is a bit of $a$ in the vector representation.

The compression map $\mathcal{C}$ described by eq. (12) costs $I_2 + M_2$ to calculate $\alpha/\beta = a + bw, a, b \in \mathbb{F}_{p^m}$ from $\alpha, \beta \in \mathbb{F}_{(p^m)^2}$. The decompression map $\mathcal{D}$ described by eq. (13) costs $3M_1$ to calculate $u(b)$. Because $u(b)$ is

$$\begin{cases} u(b) = b^{t+1} + (u_0 + u_4)b^t + (u_0 + u_3 + 1)b + (u_0u_3 + u_2 + u_6) \text{ for } G_- \\ u(b) = b^{t+1} + (u_0 + u_4)b^t + (u_0 + u_3 + 1)b + (u_0u_3 + u_2 + u_6 + 1) \text{ for } G_+ \end{cases}$$

where $u_0, u_2, u_3, u_4, u_6 \in \mathbb{F}_{p^m}$ are precomputable parameters.

We recall an estimation of exponentiation cost [13]. We determine the width-$w$ NAF representation of the power $r$, and then it contains on average $\log_2 r/(w+1)$ nonzero digits. After precomputing $g_i = g^i, i \in \{\pm 1, \pm 3, \pm 5, \cdots, \pm 2^{w-1} - 1\}$, it costs $\log_2 rS_4 + \log_2 r/(w+1)M_4$ to calculate $g^r$ on average. If we calculate in the projective representation and store results of precomputation in the $\mathbb{T}_2$ affine representation, then we can replace $M_4$ with $2M_2 = 6M_1$.

*Factor 6.* Let $\#G_\pm = p^m \pm t + 1, t = \sqrt{3p^m}, p = 3$ and $m$ be odd.

The compression map $\mathcal{C}$ is described by eq. (14) and the decompression map $\mathcal{D}$ is described by eq. (15).

$$\begin{aligned} \mathcal{C} : G_- \backslash \{1\} &\to \{0,1,2\} \times \mathbb{F}_{p^m} \\ \frac{\alpha + \beta\sigma}{\alpha - \beta\sigma} &\mapsto (i, c) \end{aligned} \tag{14}$$

$$\begin{aligned} \mathcal{D} : \{0,1,2\} \times \mathbb{F}_{p^m} &\to G_- \backslash \{1\} \\ (i, c) &\mapsto \frac{(a + bw + cw^2) + \sigma}{(a + bw + cw^2) - \sigma} \end{aligned} \tag{15}$$

Let $\mathbb{F}_{(p^m)^6} = \mathbb{F}_{(p^m)^3}(\sigma)$, $\mathbb{F}_{(p^m)^3} = \mathbb{F}_{p^m}(w)$, $\sigma \in \mathbb{F}_{(p^m)^6}, w \in \mathbb{F}_{(p^m)^3}$. We obtain $a, b, c \in \mathbb{F}_{p^m}$ by $\alpha/\beta = a + bw + cw^2$ from $\alpha, \beta \in \mathbb{F}_{(p^m)^3}$. We calculate roots of $P_6(x,c) = x^3 + 2c^{2t}x + C(c) \in \mathbb{F}_{p^m}[x]$ led by $g^{p^m - t+1} = 1$ in order to obtain $a, b$ from $c$. Where, $C(c) = \frac{2(c^{3t+3} + c^{2t} + 1)}{c^3}$. The above polynomial $P_6(x)$ has roots $\{c^tR, c^t(R+1), c^t(R-1)\}$ as $b^t$. $R$ is a solution of $x^3 - x + D(c) = 0$. Note that if the characteristic is 3, solving the above equation is easy. $a^t$ is a root of degree-1 polynomial $P_2(x) \in \mathbb{F}_{p^m}[x]$. Therefore, three solutions are $\{(a,b,c), (a-b+c, b+c, c), (a+b+c, b-c, c)\}$.

The additional information $i$ is a trit of $b$ in the vector representation. The place is the same for the least nonzero trit of $c$.

The compression map $\mathcal{C}$ described by eq. (14) costs $I_3+M_3$ to calculate $\alpha/\beta = a + bw + cw^2, a, b, c \in \mathbb{F}_{p^m}$ from $\alpha, \beta \in \mathbb{F}_{(p^m)^3}$. The decompression map $\mathcal{D}$ described by eq. (15) costs $I_1 + 7M_1 + 2S_1$ to calculate

$$D(c) = \frac{2(c^{3t+3} + c^{2t} + 1)}{c^{3t+3}}$$

and to solve the following degree-1 polynomial

$$P_2(x) = x + 2b^{2t+3} + 2b^{2t}c^3 + b^t c^{t+3} + c^{2t+3} + 2c^t \in \mathbb{F}_{p^m}[x].$$

We recall an estimation of exponentiation cost [13]. We determine the width-$w$ radix-3 NAF representation of the power $r$, and then it contains on average $2\log_3 r/(2w+1)$ nonzero digits. After precomputation, it costs $\log_3 r C_6 + 2\log_3 r/(2w+1)M_6$ to calculate $g^r$ on average. If we use the projective representation and the $\mathbb{T}_2$ affine representation, then we replace $M_6$ with $2M_3 = 12M_1$.